UNIVERSIDADE TIRADENTES

LUCIANO ALVES LUNGUINHO SANTOS

O IMPACTO DA ENGENHARIA SOCIAL NA SEGURANÇA DA INFORMAÇÃO

Aracaju

2004

LUCIANO ALVES LUNGUINHO SANTOS

O IMPACTO DA ENGENHARIA SOCIAL NA SEGURANÇA DA INFORMAÇÃO

Monografia apresentada à UniversidadeTiradentes, como pré-requisito de conclusão do curso de Pós-Graduação em redes de computadores.

MARIO VASCONCELOS

Aracaju

2004

LUCIANO ALVES LUNGUINHO SANTOS

O IMPACTO DA ENGENHARIA SOCIAL NA SEGURANÇA DA INFORMAÇÃO

Monografia apresentada à Universidade Tiradentes, como pré-requisito de conclusão do curso de Pós-Graduação em redes de computadores.

APROVADA EM :___/___/____

BANCA EXAMINADORA

____

Orientador(a)
UNIT

____

Examinador(a)
UNIT

____

Examinador(a)
UNIT

À minha esposa, por seu auxílio e paciência e aos meus filhos, simplesmente por existirem e, através de seus sorrisos, contribuírem para meu crescimento.

AGRADECIMENTOS

Para a conclusão deste trabalho foi fundamental a colaboração de:

Minha filha Jéssica cuidando de seu irmão Gustavo para que eu pudesse estudar, da minha esposa Ivânia que me motivou em meus momentos de fraqueza, dos gerentes de informática e de recursos humanos das empresas que formam o ambiente de pesquisa que, apesar de não poder citar seus nomes aqui por questões de segurança, agradeço à sua atenção e presteza, além dos usuários que forneceram as informações que formam a base deste trabalho.

Professor Ronaldo Linhares, que me orientou na fase inicial de construção deste projeto, ao professor Domingos que, na matéria de segurança em redes, abordou com competência a norma NBR ISSO 17799 e os demais assuntos que estão contidos neste trabalho, dos professores Exson, Hugo, Marco Simões e Othon que contribuíram excelentemente com o meu aprendizado e, conseqüentemente, com o meu desenvolvimento profissional e do professor Mário Vasconcelos que ampliou a minha visão deste trabalho ao mesmo tempo em que me motivou durante todo o processo de desenvolvimento do mesmo, sempre com atenção e simpatia.

Agradeço a todos que contribuíram direta ou indiretamente durante todo o projeto, desde as aulas iniciais do curso até as últimas linhas desta monografia.

"Mentes grandes discutem idéias; mentes medianas discutem eventos; mentes pequenas discutem pessoas".

Blaise Pascal
físico, matemático e filósofo
FRA, 1623-1662....

RESUMO

O principal objetivo deste trabalho é criar uma metodologia para diagnosticar a consciência dos usuários quanto ao risco de ataques de engenharia social no ambiente corporativo e saber qual o nível de conscientização de seus colaboradores quanto a confidencialidade, integridade e disponibilidade da informação. Para isso dividimos o trabalho em basicamente três etapas: A pesquisa, a tabulação e análise dos dados e a proposta de soluções. Antes de abordarmos a metodologia, iniciamos com um nivelamento de conceitos, definindo o que vem a ser informação e engenharia social, como ela funciona e qual o papel do usuário na segurança da informação. Visando uma abordagem sistêmica, a pesquisa foi feita com os usuários, com o setor de recursos humanos e com a área responsável pela tecnologia da informação, com questionários criados para abordar os principais pontos da engenharia social como por exemplo a confidencialidade de senhas. Aplicamos os questionários em empresas com modelos administrativos distintos, sendo uma da administração pública e a outra, uma empresa privada. Após a tabulação dos dados, analisamos os principais pontos, cruzando respostas dos três questionários, analisando de acordo com o tipo da empresa, se o usuário é da área gerencial, operacional ou é um usuário temporário, como por exemplo um terceirizado ou um estagiário. Finalmente, utilizando como base os questionamentos elencados na metodologia e o resultado da análise, elaboramos uma proposta com sugestões de implementação de controles e ações para minimizar os riscos de ataques de engenharia social. Para isso utilizamos controles que achamos mais relevantes no tratamento dos riscos de ataques de engenharia social existentes na

norma ISO/IEC 17799 - Código de Prática para Gestão da segurança da Informação nas Empresas.

LISTAS

LISTAS DE FIGURAS

LISTAS DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

> “Homo homini lupus: O homem é o lobo do homem. Das palavras do dramaturgo Plauto, resgatadas pelos filósofos Francis Bacon e Thomas Hobbes, temos o mote para uma das maiores preocupações em termos de segurança: como prevenir as pessoas contra as próprias pessoas.” [7]

Os fatores humanos sempre ficam, naturalmente, em segundo plano, quando existem diversos aparatos tecnológicos de última geração para garantir a segurança. Porém, deixar as pessoas desinformadas sobre as questões de segurança pode expor uma organização a riscos desnecessários, uma vez que os “invasores” utilizam a habilidade de enganar os usuários, alinhada à inclinação natural das pessoas de confiar uma nas outras e de querer ajudar, para persuadi-las a abrir-lhes a “porta de entrada”, quebrando a segurança da informação através da exploração de falhas ou, pior ainda, do próprio nome e senha do *usuário*.

Por sermos humanos, seres imperfeitos, modificamos nosso comportamento natural em situações de riscos, fazendo com que, inconscientemente, tomemos decisões baseados em confiança e no grau de criticidade da situação, permitindo assim que o *engenheiro social* possa explorar de maneira eficaz nossas falhas para burlar a segurança da informação.[7]

Um dos principais problemas que a segurança da informação deve tratar é a segurança em pessoas. A cooperação dos usuários é essencial para a eficácia da segurança. Eles exercem um forte impacto sobre a confidencialidade, a

integridade e a disponibilidade da informação, pois, por exemplo, o *usuário* que não mantiver a confidencialidade da senha, não evitar o registro da mesma em papéis que não estão guardados em locais seguros, não utilizar senhas de qualidade ou ainda que compartilha senhas individuais, compromete a segurança da informação.

Chamamos de Engenharia social a habilidade de enganar um ou mais usuários para quebrar a segurança da informação. Ela é um perigo real e sutil e é fundamental que as organizações assegurem-se que seus usuários sejam atuantes defensores da sua informação e que não sejam facilmente ludibriados por pessoas mal intencionadas e não autorizadas, abrindo assim o caminho para o acesso a informação. Por esses e outros motivos, antes de qualquer coisa, todos os usuários devem saber o que é a informação para sua empresa, qual a sua importância e por que a segurança da informação é fundamental.

A segurança da informação pode ser caracterizada pela preservação de três fatores [14]:

- **Confidencialidade**: Garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
- **Integridade**: Exatidão, completeza da informação e dos métodos de processamento;
- **Disponibilidade**: Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

A informação de uma empresa é o seu principal patrimônio. O código de prática para a gestão da segurança da informação diz que:

> "A informação é um ativo que, como qualquer outro, importante para os negócios, tem um valor para a organização. A segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos ao negócio e maximizar o retorno dos investimentos e as oportunidades de negócios".
>
> (NBR ISO/IEC 17799:2001, pág. 2).

Este trabalho visa avaliar a consciência que os usuários possuem sobre a segurança da informação, sugerindo ações para evitar problemas com a engenharia social e orientar a implementação de controles de segurança em pessoas no ambiente estudado.

1.1. JUSTIFICATIVA

A informação de uma empresa é o seu principal patrimônio, fundamental para o seu funcionamento, garantindo a competitividade no mercado. Por conta disso, concorrentes, utilizando-se da engenharia social, podem vir a obter informações confidenciais sobre a estratégia, metas e planejamento.

Com base nisso propomos às empresas que tenham o interesse de avaliar a segurança da informação, no que diz respeito à engenharia social, seguir a metodologia utilizada aqui como base para implementação de controles que minimizem as falhas no acesso à informação, aumentando a segurança nas pessoas e conscientizando seus usuários da importância da informação da empresa, tornando-os um “agente” da segurança da informação, cumprindo o seu papel e suas obrigações de, por exemplo, manter a sua senha segura.

A sociedade que possuir pessoas que tenham o devido cuidado com a informação será uma sociedade mais segura, pois será muito mais difícil utilizar a engenharia social para conseguir burlar a segurança da informação, seja ela de uma empresa, da conta bancária de um *usuário* ou de um projeto comunitário importante, evitando assim golpes que venham a lesar alguém desta comunidade.

Este projeto tem o intuito de, baseando-se em um estudo de caso real, criar uma orientação dos passos para tratar o problema da engenharia social, prevenindo que pessoas não autorizadas utilizem os usuários desinformados e desatentos para conseguir acesso a informações importantes.

1.2. OBJETIVOS

1.2.1. OBJETIVO GERAL

- Desenvolver um procedimento que nos permita, através da aplicação de questionários, conhecer as falhas que podem ser utilizadas pela engenharia social para quebrar a segurança da informação em instituições com características diferentes, propondo soluções para estas falhas.
-

1.2.2. OBJETIVOS ESPECÍFICOS

- Avaliar a consciência dos usuários sobre a importância da informação que eles têm acesso e sobre o problema da engenharia social, através de pesquisa aplicada ;

- Propor melhorias nos processos que envolvem o RH e a engenharia social;

- Sugerir a implementação de controles e ações para minimizar os riscos de ataque de engenharia social;

- Servir como modelo na prevenção do problema de engenharia social, desenvolvendo um procedimento para avaliação da consciência dos usuários sobre o referido problema.

2. ENGENHARIA SOCIAL

Antes de entendermos como a engenharia social funciona, é fundamental que conheçamos seu conceito, bem como o conceito de informação.

2.1. CONCEITO DE INFORMAÇÃO

Podemos dizer que Informação é um processo que visa o conhecimento, ou, mais simplesmente, “Informação é tudo o que reduz a incerteza. Um instrumento de compreensão do mundo e da ação sobre ele" [10].

Toda informação está associada a um dado ou valor representando o suporte lógico para a mesma. É o uso que será feito deste dado e dos conceitos a ele relacionados, que o torna útil ou não.

A informação desempenha um papel estratégico dentro das organizações, tornando-se uma necessidade crescente e indispensável para qualquer setor da atividade humana. Justamente por isso, surge a preocupação em garantir a sua segurança e protegê-la de acessos indevidos. Sendo assim, seja qual for a forma que a informação é apresentada (impressa, escrita, falada, entre outras) faz-se necessário que ela seja sempre protegida adequadamente.

Independente do meio em que a informação circula, ela sempre é destinada a pessoas, que a priori podem e devem acessa-las. É exatamente este o alvo da engenharia social.

2.2. DEFINIÇÃO DE ENGENHARIA SOCIAL

A arte de trapacear, construir métodos e estratégias de enganar em cima de informações cedidas por pessoas ou ganhar a confiança para obter informações, são ações antigas, oriundas dos tempos mais remotos, ganharam um novo termo: Engenharia Social.

Engenharia por que constrói, em cima de informações, táticas de acesso a sistemas e informações sigilosas, de forma indevida. Social por que se utiliza de pessoas que trabalham e vivem em grupos organizados.

Podemos dizer que a engenharia social é um tipo de ataque utilizado por *hackers*, onde a principal "arma" utilizada é a habilidade de lhe dar com pessoas, induzindo-as a fornecer informações, executar programas e muitas vezes, fornecer senhas de acesso.

> "A segurança compreende três componentes – pessoas, processos e tecnologia –, e o resultado final deve ser a preservação da confiança". MCCARTTHY e CAMPBELL (2003, p. 44), citando MacLean, a vice-presidente sênior e diretora de proteção da informação do Bank of América.

A engenharia social visa explorar as pessoas no intuito de ocasionar a perda, a indisponibilidade ou a violação da informação. Ela vai diretamente para o elo mais fraco de qualquer sistema de segurança: pessoas. O chamado *engenheiro*

social utiliza a sua criatividade, poder de persuasão e habilidade, para envolver a vítima em uma situação onde, muitas vezes, ela nem percebe que abriu as “portas” para um invasor.

O “ataque” do *engenheiro social* pode ocorrer através de um bom papo, numa mesa de bar, ao telefone ou, em casos mais sofisticados, através da sedução. O sucesso deste “ataque” esta no fato de o *usuário* abordado nem seque se dar conta do que acabou de acontecer. Ou seja, o engenheiro social, além de obter a informação que deseja ainda mantém as “portas” abertas com o seu “informante”.

Os alvos principais são os usuários detentores de privilégios equivalentes aos dos chefes como, por exemplo, auxiliares e secretários, que muitas vezes têm acesso ao correio eletrônico, aos sistemas gerenciais e sabem até a senha utilizada pelo seu superior.

> “Geralmente as pessoas são o ponto mais suscetível em um esquema de segurança. Um trabalhador malicioso, descuidado ou alheio à política de informação de uma organização pode comprometer até a melhor segurança.” (COMMER 1988, p. 525)

A falta de consciência das técnicas de engenharia social utilizadas e o excesso de autoconfiança das pessoas (por não se considerarem ingênuas e acharem que não podem ser manipuladas) são os principais fatores que favorecem ao sucesso da Engenharia Social.

2.3. COMO FUNCIONA A ENGENHARIA SOCIAL

Muitos são os meios e técnicas para se obter acesso indevido à informação, esteja ela em formato eletrônico, em papel ou em outros formatos. A engenharia social é muito utilizada para o levantamento de informações preliminares que possam tornar a tentativa de invasão mais eficiente.

Um ataque de engenharia social pode ser feito através e–mail, telefone, fax, Chat e até, em último caso, pessoalmente. A ingenuidade ou a confiança de um *usuário* é utilizada pelos engenheiros sociais para se conseguir informações, que muitas vezes parecem sem importância, mas que nas mãos erradas podem causar bastante estrago.

Uma das táticas fundamentais de engenharia social é obter acesso a informações que os funcionários da empresa tratam como inofensivas e utilizá-las para ganhar a confiança de outros usuários e conseguir as informações que ele realmente deseja.[8]

Muitos acreditam que os engenheiros sociais utilizam ataques com mentiras elaboradas bastante complexas, porém, muitos ataques são diretos, rápidos e muito simples, onde eles simplesmente pedem a informação desejada.

Os grupos de atacantes não se restringem a pessoas externas à empresa, pois, visto que a motivação, a habilidade e a oportunidade são essenciais a um atacante que deseja ter acesso à informação de uma empresa, (ex) funcionários e (ex) contratados são os mais perigosos grupos de atacantes, pois eles são capacitados pelas empresas para dominarem as habilidades e, muitas

vezes eles se sentem frustrados, o que pode ser um motivo para idealizarem um ataque. Sendo eles conhecidos e se transmitem confiança a outros funcionários, ou pior, se ainda fazem parte do quadro funcional da empresa, eles possuem a oportunidade necessária para um ataque [3].

> "*Geralmente as pessoas são o ponto mais suscetível em um esquema de segurança. Um trabalhador malicioso, descuidado ou alheio à política de informação de uma organização pode comprometer até a melhor segurança." (COMMER 1988, p. 525).*

As técnicas mais costumeiras, que podem ser usadas de maneira individual ou combinadas, são: [7]

- Contatos telefônicos, simulando atendimento de suporte ou uma ação de emergência;
- Contato através de e-mail, atuando como estudante com interesse em pesquisa sobre determinado assunto ou como pessoa com interesse específico em assunto de conhecimento da vítima;
- Contato através de ferramentas de Instant Messaging (Yahoo Messenger, MS Messenger, Mirabilis ICQ, etc), simulando pessoa com afinidades com a vítima;
- Obtenção de informações vazadas por parte da administração de rede e funcionários em geral em listas de discussão ou comunidades virtuais na Internet, o que motivaria também um contato posterior mais estruturado;
- Uso de telefone público, para dificultar detecção;
- Varredura do lixo informático, para obtenção de informações adicionais para tentativas posteriores de contato;
- Disfarce de equipe de manutenção;

- Visita em pessoa, como estudante, estagiário ou pessoa com disfarce de ingenuidade.

2.4. A SEGURANÇA E O USUÁRIO

É indiscutível que todos os usuários desejam segurança, porém quando eles têm que interagir com ela e tomar decisões baseando-se em procedimentos de segurança, a maioria acha que ela atrapalha. É comum que usuários nem pensem duas vezes para contornar os procedimentos de segurança em determinadas situações, como por exemplo quando se aproxima um prazo para entrega de um trabalho importante. Eles podem desativar um firewall ou até mesmo fornecer uma senha, pois o trabalho precisa ser feito.[12]

Os engenheiros sociais sabem que esta maneira de agir dos usuários e exploram este comportamento criando este tipo de situação para que a segurança seja quebrada.

2.5. EXEMPLOS DE ATAQUES

A engenharia social também pode ser utilizada como tática no terrorismo físico. O mundo presenciou os ataques à Nova York (World Trade Center) e Washington D.C. em setembro de 2001 que imputaram tristeza e medo em nossos corações, aumentando temporariamente os níveis de nossa consciência de segurança, e nos colocando em alerta quanto à ação do terrorismo no mundo. Porém, a consciência deste perigo deve permanecer conosco, visto, por exemplo,

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

que os terroristas utilizam identidades falsas, assumem os papeis de alunos e vizinhos, misturando-se à multidão enquanto conspiram contra as pessoas e escondem suas verdadeiras crenças e intenções.

Estão cada vez mais comuns notícias de tentativas de fraude utilizando diversos meios de comunicação, onde a Internet é o mais popular, sendo registrado pelo NIC BR Security Office (NBSO), grupo brasileiro de resposta a incidentes de segurança, 1.358 incidentes envolvendo fraudes pela Internet somente nos últimos 6 meses [15]. Um dos principais alvos dos fraudadores é o *internet banking*. Eles utilizam, além de outras técnicas, a engenharia social para, por exemplo, tentar se passar por funcionários de confiança do banco, como um gerente ou o administrador do site, ou ainda, enviam um link por e-mail que aponta para o site clonado de um banco, na tentativa de fazer o usuário digitar seus dados, inclusive a sua senha.

Além das fraudes, os vírus, *spywares* e outros *malwares*, utilizam a engenharia social tentando diversos truques para persuadir as pessoas a abri-los. Os *Cavalos de Tróia*, por exemplo, necessitam da intervenção de um usuário para que possam atingir seus objetivos.

Além dos ataques que utilizam tecnologias como Internet, e-mails e programas de Chats, muitas informações são conseguidas em documentos impressos, até mesmo no lixo, e em entrevistas para emprego, onde os engenheiros sociais, por exemplo, fingem interesse em uma vaga e participam da seleção somente para levantar informações para um concorrente.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

3. METODOLOGIA

Para entender como as empresas tratam do assunto “engenharia social”, desenvolvemos um procedimento para aplicação de uma pesquisa descritiva com questões relativas à Segurança da Informação. A idéia central desta pesquisa consiste em identificar como o ambiente estudado trata suas informações e qual o nível de conscientização de seus colaboradores quanto a confidencialidade, integridade e disponibilidade da informação.

Para tal, foram elaborados 03 (três) instrumentais de pesquisas (vide anexos I,II e III), sendo o Questionário I direcionado a todos os colaboradores do escopo, com acesso a computadores, abrangendo todos os cargos, o Questionário II destinado ao setor de Recursos Humanos e o Questionário III, destinado ao setor de Informática.

Em todos os questionários foram abordadas questões direcionadas a senhas, tipos de informações que circulam pela empresa, existência de uma política de comunicação interna e externa, *política de segurança*, dentre outras questões relevantes para identificação dos pontos mais críticos que refletem o nível de conscientização dos usuários, quanto à Segurança da Informação.

O primeiro passo é a pesquisa aplicada, que visa conhecer como está a consciência dos funcionários. Esta pesquisa tem o intuito de levantar se os usuários têm consciência do valor da informação, se eles sabem quais podem ser disseminadas e quais não podem ser discutidas fora do ambiente “seguro”, que é o

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

seu grupo de trabalho, se existe uma cultura de divulgação de ações de segurança como política de utilização de senhas, de e-mails, termos de confidencialidade e responsabilidade, entre outros.

O Questionário do ANEXO I foi elaborado visando permitir identificar se os usuários têm consciência da engenharia social e de seus riscos, se suas senhas são realmente individuais, se confiam em todas as informações que chegam por e-mail, se existe uma *política de segurança* conhecida na empresa, quais os sistemas utilizados, se trabalham em outras empresas atuantes na mesma área da empresa pesquisada, entre outros.

Em paralelo com a pesquisa dos usuários, os processos que envolvem o setor de recursos humanos e de tecnologia da informação com a engenharia social, tais como de admissão e demissão, devem ser re-avaliados visando identificar oportunidades de melhorias e a integração dos processos de ambos os setores, como por exemplo no caso da demissão de um funcionário, onde o setor de *TI* deve ser informado imediatamente para cancelamento de todos os acessos à rede e aos sistemas. Foi com esse intuito que os questionários dos ANEXO II e III foram elaborados: Padronizar o levantamento das informações no setor de recursos humanos e de informática.

Após a tabulação dos dados, deve-se analisar a pesquisa, levantando os pontos fortes e fracos em relação à consciência da importância da segurança da informação. Visando facilitar esta análise, sugerimos caracterizar em três grupos identificados aqui como:

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

1. **Gerencial**: Composto pelos principais líderes da organização. Estes usuários detêm acesso às principais informações da empresa. São conhecedores das estratégias utilizadas para alcançar as metas da instituição, dos e projetos existentes e dos indicadores de desempenho estratégicos.

2. **Operacional**: São os técnicos que possuem conhecimentos específicos dos processos de cada área e têm acesso aos sistemas que fornecem a informação para tomadas de decisão. Estão incluídos os agentes administrativos, os oficiais administrativo, os auxiliares de Gabinete entre outros.

3. **Temporário**: São usuários prestadores de serviços e estagiários que, em sua maioria, acabam saindo da empresa com informações importantes.

A Análise da pesquisa deve cruzar as informações colhidas nos três questionários, buscando responder os questionamentos abaixo:

1. A empresa possui uma *política de segurança* da informação amplamente divulgada aos seus usuários?
2. Das pessoas que acessam informações confidenciais, quantas sabem se a empresa possui política de comunicação interna?
3. Quantos usuários sabem quais as informações vitais para a empresa, por grupo?

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

4. Se os funcionários assinam algum termo de responsabilidade e/ou de confidencialidade sobre as informações da empresa?

5. Das pessoas que acessam informações confidenciais, quantas sabem se a empresa possui responsável pela comunicação externa e interna?

6. Das pessoas que acessam informações confidenciais, quantas sabem se a empresa orienta quanto a divulgação de informações?

7. Qual a freqüência de alteração de senhas das pessoas que acessam informações confidenciais?

8. Quantos usuários divulgam suas senhas?

9. Quantos usuários permitem que outros utilizem suas senhas?

10. Quantos usuários anotam suas senhas em locais que podem não ser seguros?

11. Quais sistemas têm usuários que divulgam ou anotam suas senhas?

12.Os usuários bloqueiam seus computadores ao sair e fazem a política de mesa limpa?

13. O setor de RH contribui para a segurança da informação?

14. Existe restrição quanto a utilização de e-mail, Internet e telefone?

15. Quais os principais controles utilizados pelo setor de informática para minimizar os riscos de acessos indevidos à informação?

16. Os setores de RH e informática trabalham integrados para garantir a segurança da informação?

17. Existe controle de acesso aos prestadores de serviço/Terceirizados?

Esses questionamentos formam a base para o dimensionamento do impacto da engenharia social na segurança da informação, avaliando a consciência

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

dos usuários sobre a importância da informação que eles têm acesso e sobre o problema da engenharia social.

Finalmente, elabora-se uma proposta contendo melhorias nos processos que envolvem o RH, a Tecnologia da Informação e a engenharia social, com sugestões de implementação de controles e ações para minimizar os riscos de ataque de engenharia social;

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

4. ESTUDO DE CASO

4.1. CARACTERIZAÇÃO DAS INSTITUIÇÕES ESTUDADAS

Por questões de segurança e privacidade, os nomes das empresas, bem como outras informações sigilosas serão preservadas, evitando assim que estas sejam utilizadas indevidamente em possíveis ataques. As empresas serão identificadas aqui como “Pública” e “Privada”.

4.1.1. APLICAÇÃO DOS QUESTIONÁRIOS

Ao todo foram respondidos 91 questionários, sendo 47 da empresa Pública e 44 da empresa Privada, conforme quadro abaixo:

	EMPRESA PÚBLICA	EMPRESA PRIVADA	TOTAL	% EMPRESA PÚBLICA*	% EMPRESA PRIVADA*
QUESTIONÁRIO I (Funcionários)	45	42	**87**	**51,72 %**	**48,27 %**
QUESTIONÁRIO II (Recursos humanos)	01	01	**2**	**50 %**	**50%**
QUESTIONÁRIO III (Informática)	01	01	**2**	**50%**	**50%**
TOTAL	47	44	91	48,36%	51,64 %

* Percentual em relação ao total de questionários

Tab 1. Quantidade de questionários por empresa

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

4.1.2. EMPRESA PÚBLICA

Trata-se de um órgão integrante da Administração Estadual Direta, tendo como propósito fomentar a política governamental para o desenvolvimento econômico do estado de Sergipe.

Atualmente possui 67 funcionários, incluindo estagiários e terceirizados, dos quais foram entrevistados todos os usuários que fazem parte do escopo, num total de 45 (quarenta e cinco), sendo que:

- 53,33% possuem mais de 40 anos;

- 31,11% não possui mais do que 1 (um) ano de trabalho na empresa;

- 28,89% trabalha nela há mais de 10 anos;

- 22,22% possui outro emprego, dos quais 8,89% é na mesma área em que trabalha na empresa;

- 62,22% é do sexo feminino;

Os usuários do escopo estão distribuídos por função, de acordo com a figura abaixo:

Função	Quantidade.	%
Gerencial	12	26,67%
Operacional	22	48,89%
Terceirizado	7	15,56%
Sem resposta	4	8,89%
TOTAL.	**45**	**100%**

Tab 2. Distribuição dos usuários por função – Pública

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

4.1.3. EMPRESA PRIVADA

Trata-se de uma instituição que tem o propósito de atuar na área de saúde em todo estado de Sergipe, destacando-se também em ações para o desenvolvimento de programas sociais.

Atualmente possui 142 funcionários, incluindo estagiários e terceirizados, dos quais foram entrevistados 42 (Quarenta e dois) usuários, sendo que somente 2,38% tem menos de 21 anos e 47,62% é do sexo feminino, distribuídos por função, de acordo com a tabela abaixo:

Função	Quantidade.	%
Gerencial	6	14,29%
Operacional	24	57,14%
Terceirizado	5	11,90%
Sem resposta	7	16,67%
TOTAL.	**42**	**100%**

Tab 3. Distribuição dos usuários por função - Privada

O escopo do projeto compreende todos os usuários de informática da empresa Pública, e uma amostra de usuários da empresa Privada de maneira que todas as áreas foram abrangidas. Qualquer funcionário deste universo que tiver acesso à rede e às informações contidas em seus principais sistemas foi entrevistado e faz parte deste projeto.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

Atualmente as empresas estudadas possuem a seguinte estrutura:

Empresa	Nº de Computadores	Nº de Funcionários	Funcionários por Máquina
Pública	24	67	2,79
Privada	104	142	1,36
TOTAL	128	209	1,6

Tab 4. Usuários e Computadores

4.2. PESQUISA APLICADA

4.2.1. TABULAÇÃO DO QUESTIONÁRIO DOS USUÁRIOS

A seguir demonstramos a tabulação do questionário aplicado a todos os usuários de informática do ambiente estudado, estratificado por tipo de empresa,

4.2.2. SOBRE O FUNCIONÁRIO

1.Faixa etária

Faixa etária	Publica	Privada	TOTAL
Até 20 Anos	2,22%	2,38%	2,30%
De 21 a 30 anos	22,22%	45,24%	33,33%
De 31 a 40 anos	22,22%	45,24%	33,33%
Acima de 40 anos	53,33%	7,14%	31,03%
Não Respondeu	0,00%	0,00%	0,00%
TOTAL	100%	100%	100%

Tab 5. Faixa Etária

2.Sexo

Sexo	Publica	Privada	TOTAL
Masculino	28,89%	35,71%	32,18%
Feminino	62,22%	47,62%	55,17%
Não respondeu	8,89%	16,67%	12,64%
TOTAL	100%	100%	100%

Tab 6. Sexo

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

3.Função

Função na Empresa	Publica	Privada	TOTAL
Gerencial	26,67%	14,29%	20,69%
Operacional	49%	57,14%	52,87%
Terceirizado	16%	11,90%	13,79%
Não Respondeu	8,89%	16,67%	12,64%
TOTAL	100%	100%	100%

Tab 7. Função

4.Trabalha na empresa a

Anos de Trabalho na empresa	Publica	Privada	TOTAL
Menos de 1 ano	31,11%	28,57%	29,89%
De 1 a 5 anos	22,22%	50,00%	35,63%
De 6 a 10 anos	6,67%	4,76%	5,75%
Acima de 10 Anos	28,89%	11,90%	20,69%
Não respondeu	11,11%	4,76%	8,05%
TOTAL	100%	100%	100%

Tab 8. Tempo de empresa

5.Possui outro emprego?

Possui outro Emprego	Publica	Privada	TOTAL
Sim, na mesma área em que trabalho na EMPRESA	8,89%	0,00%	4,60%
Sim, em outra área	13,33%	9,52%	11,49%
Não	51,11%	69,05%	59,77%
Não respondeu	26,67%	21,43%	24,14%
TOTAL	100%	100%	100%

Tab 9. Possui outro emprego

4.2.3. SOBRE SENHAS

6.Alguém, além de você, sabe a(s) sua(s) senha(s) utilizada(s) para acessar informações da empresa?

Alguém mais sabe sua senha	Publica	Privada	TOTAL
Sim	11,11%	4,76%	8,05%
Não	84,44%	90,48%	87,36%
Não respondeu	4,44%	4,76%	4,60%
TOTAL	100%	100%	100%

Tab 10. Senha aberta

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

7.Você utiliza a senha de algum outro funcionário para acesso a informações da empresa?

Sabe a senha de outro usuário	Publica	Privada	TOTAL
Sim	15,56%	11,90%	13,79%
Não	73,33%	85,71%	79,31%
Não respondeu	11,11%	2,38%	6,90%
TOTAL	100%	100%	100%

Tab 11. Senha de terceiros

8.Você anota as suas senhas em algum local próximo ao computador, na agenda, ou local similar?

Anota Senha	Publica	Privada	TOTAL
Sim	6,67%	7,14%	6,90%
Não	82,22%	92,86%	87,36%
Não respondeu	11,11%	0,00%	5,75%
TOTAL	100%	100%	100%

Tab 12. Anota Senha

9.Você deixa outras pessoas utilizarem sua senha para algum trabalho rápido?

Trabalho Rápido	Publica	Privada	TOTAL
Sim	33,33%	30,95%	32,18%
Não	57,78%	66,67%	62,07%
Não respondeu	8,89%	2,38%	5,75%
TOTAL	100%	100%	100%

Tab 13. Cede em caso de trabalhos rápidos

10.Com que freqüência você altera (s) sua(s) senha(s):

Freqüência que Altera Senhas	Publica	Privada	TOTAL
Mensalmente	2,22%	0,00%	1,15%
Trimestralmente	6,67%	2,38%	4,60%
Semestralmente	4,44%	2,38%	3,45%
Somente quando o sistema solicita alteração	64,44%	35,71%	50,57%
Sempre utilizo a mesma senha	20,00%	59,52%	39,08%
não respondeu	2,22%	0,00%	1,15%
TOTAL	100%	100%	100%

Tab 14. Freqüência de alteração de senhas

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

4.2.4. SOBRE DIVULGAÇÃO DE INFORMAÇÕES

11.Como você procede para fornecer informações, que você tem acesso, solicitadas por telefone ou e-mail?

Fornece informações por telefone	Publica	Privada	TOTAL
Não respondeu	2,22%	2,38%	2,30%
Forneço a informação, pois não há nada confidencial em minha área	4,44%	4,76%	4,60%
Forneço a informação, após identificar o solicitante	33,33%	47,62%	40,23%
Solicito autorização ao meu superior para liberar a informação	57,78%	33,33%	45,98%
Outros	6,67%	14,29%	10,34%
TOTAL	100%	100%	100%

Tab 15. Informações por telefone

<table>
<tr><th>Fornece Informações por telefone - outros</th><th>Empresa</th></tr>
<tr><td>Depende do tipo de informação solicitada</td><td rowspan="3">Pública</td></tr>
<tr><td>Não forneço</td></tr>
<tr><td>NÃO ESPECIFICOU</td></tr>
<tr><td>Minha prática é fornecer informações por escrito e não por telefone, autorizado pelo Gestor</td><td rowspan="6">Privada</td></tr>
<tr><td>Só dou informações aos gestores da empresa</td></tr>
<tr><td>Depende de quem seja o solicitante, qual informação solicitada e se foi liberado pelo coordenador</td></tr>
<tr><td>Forneço somente quando a informação não for confidencial</td></tr>
<tr><td>Só forneço a partir de quando ele pede somente para confirmar os dados</td></tr>
<tr><td>Depende da informação</td></tr>
</table>

Tab 16. Outras respostas - Informações por telefone

4.2.5. SOBRE A EMPRESA

12.A Empresa possui política de comunicação interna?

Política de Comunicação Interna	Publica	Privada	TOTAL
Sim	64,44%	73,81%	68,97%
Não	24,44%	9,52%	17,24%
Não respondeu	11,11%	16,67%	13,79%
TOTAL	100%	100%	100%

Tab 17. Política de comunicação interna

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

13.As informações são classificadas na Empresa (confidencial, secreta, pública etc....)

As informações são classificadas	Publica	Privada	TOTAL
Sim	37,78%	40,48%	39,08%
Não	42,22%	40,48%	41,38%
Não respondeu	20,00%	19,05%	19,54%
TOTAL	100%	100%	100%

Tab 18. Classificação de informações

14.A Empresa possui um responsável pela comunicação externa?

Há um responsável pela comunicação Externa	Publica	Privada	TOTAL
Sim	55,56%	66,67%	60,92%
Não	24,44%	21,43%	22,99%
Não respondeu	20,00%	11,90%	16,09%
TOTAL	100%	100%	100%

Tab 19. Comunicação Externa

15.A Empresa possui alguma orientação quanto à divulgação de informação?

Orientado quanto à divulgação de informações	Publica	Privada	TOTAL
Sim	42,22%	71,43%	56,32%
Não	37,78%	19,05%	28,74%
Não respondeu	20,00%	9,52%	14,94%
TOTAL	100%	100%	100%

Tab 20. Divulgação de informações

16.Você sabe quais as informações são vitais para o negócio da empresa?

Sabe quais são as informações Vitais para a empresa	Publica	Privada	TOTAL
Sim	40,00%	59,52%	49,43%
Não	44,44%	28,57%	36,78%
Não respondeu	15,56%	11,90%	13,79%
TOTAL	100%	100%	100%

Tab 21. Informações vitais

17.A empresa possui política de segurança da informação?

Existe uma política segurança	Publica	Privada	TOTAL
Sim	42,22%	40,48%	41,38%
Não	42,22%	35,71%	39,08%
Não respondeu	15,56%	23,81%	19,54%
TOTAL	100%	100%	100%

Tab 22. Política de segurança da informação

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

4.2.6. SOBRE ACESSO À INFORMAÇÃO

18.Neste momento existe algum papel sobre sua mesa com informações sobre a empresa?

Há papel na mesa com informações da empresa	Publica	Privada	TOTAL
Sim	46,67%	40,48%	43,68%
Não	44,44%	50,00%	47,13%
Não respondeu	8,89%	9,52%	9,20%
TOTAL	100%	100%	100%

Tab 23. Papel na mesa

19.Ao sair você costuma deixar suas mesa limpa, sem papéis?

Mesa_Limpa/Empresa	Publica	Privada	TOTAL
Sim	77,78%	69,05%	73,56%
Não	20,00%	30,95%	25,29%
Não respondeu	2,22%	0,00%	1,15%
TOTAL	100%	100%	100%

Tab 24. Política de mesa limpa

20.Ao sair você costuma deixar seu computador bloqueado ou efetuar o LogOff?

Bloqueia Equipamento	Publica	Privada	TOTAL
Sim	86,67%	71,43%	79,31%
Não	8,89%	23,81%	16,09%
Não respondeu	4,44%	4,76%	4,60%
TOTAL	100%	100%	100%

Tab 25. Bloqueio de estações de trabalho

21.O seu setor possui informações consideradas confidenciais?

Setor com Informações Confidenciais	Publica	Privada	TOTAL
Sim	75,56%	71,43%	73,56%
Não	22,22%	23,81%	22,99%
Não respondeu	2,22%	4,76%	3,45%
TOTAL	100%	100%	100%

Tab 26. informações confidenciais

22.Na sua opinião, todos os funcionários do seu setor sabem a importância das informações da empresa?

Sabem a Importância das Informações	Publica	Privada	TOTAL
Sim	62,22%	78,57%	70,11%
Não	31,11%	16,67%	24,14%
Não respondeu	6,67%	4,76%	5,75%
TOTAL	100%	100%	100%

Tab 27. Consciência da importância da informação

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

23.Na sua opinião, seria difícil pessoas externas conseguirem informações importantes na empresa?

É difícil pessoas Externas conseguirem informações	Publica	Privada	TOTAL
Sim	53,33%	45,24%	49,43%
Não	33,33%	47,62%	40,23%
Não respondeu	13,33%	7,14%	10,34%
TOTAL	100%	100%	100%

Tab 28. Acesso á informação por pessoas externas

24.Quais os tipos de informações que você tem acesso?

Tipo de informações que tem acesso	Publica	Privada	TOTAL
Informações operacionais	66,67%	92,86%	79,31%
Informações Gerenciais	31,11%	47,62%	39,08%
Informações Confidenciais da Empresa	28,89%	30,95%	29,89%
Informações imprescindíveis à continuidade do negócio da Empresa	22,22%	23,81%	22,99%
Não tenho acesso a nenhuma informação importante	22,22%	4,76%	13,79%
Não respondeu	2,22%	0,00%	1,15%
TOTAL	100%	100%	100%

Tab 29. Acesso por tipo de informação

4.2.7. SOBRE OS SISTEMAS UTILIZADOS

25.Dos sistemas abaixo, quais você utiliza?

Sistemas que utiliza	Publica	Privada	TOTAL
Não respondeu	22,22%	16,67%	19,54%
Sistema de ponto	22,22%	50,00%	35,63%
Sistema Financeiro/Contábil	22,22%	19,05%	20,69%
Sistema de patrimônio	2,22%	4,76%	3,45%
Folha de pagamento	17,78%	14,29%	16,09%
Sistema orçamentário	17,78%	4,76%	11,49%
Sistema com informações gerenciais	8,89%	28,57%	18,39%
Outros	35,56%	11,90%	24,14%
TOTAL	100%	100%	100%

Tab 30. Sistemas utilizados

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

4.3. TABULAÇÃO DO QUESTIONÁRIO DO RH

4.3.1. SOBRE A CONTRATAÇÃO DE FUNCIONÁRIOS

1. A política de segurança da informação é divulgada aos novos contratados?

Empresa	Resposta
Publica	Não
Privada	Sim

Tab 31. Novos contratados - RH

2. Os funcionários assinam algum termo de responsabilidade e/ou de confidencialidade sobre as informações da empresa?

Empresa	Resposta
Publica	Não
Privada	Não

Tab 32. Termo de confidencialidade - RH

3. Existe alguma orientação de restrição quanto à utilização de e-mail, Internet ou telefone?

Empresa	Resposta
Publica	Sim, através do servidor da redes e da central telefônica;
Privada	Outros

Tab 33. Orienta utilização de e-mail, Internet ou telefone **- RH**

4. Em caso de outros, qual?

Empresa	Resposta
Publica	
Privada	Divulgação da melhor forma de utilizar as ferramentas Intranet, e-mail e Internet por parte da assessoria de informática.

Tab 34. Orienta utilização de e-mail, Internet ou telefone **/outros - RH**

5. As informações (geralmente contidas no currículo) dos candidatos, fornecidas no processo de seleção, são checadas antes da contratação?

Empresa	Resposta
Publica	Outros
Privada	Sim

Tab 35. Checa currículos- RH

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

6. Em caso de outros, qual?

Empresa	Resposta
Publica	Contrato ou decreto são feitos pela secretaria de estado da administração.
Privada	

Tab 36. Checa currículos/outros - RH

7. Os funcionários recém contratados ...

Empresa	Resposta
Publica	São encaminhados diretamente à TI para cadastro na rede e demais sistemas.
Privada	Aguardam o processo de criação de e-mail após um documento ser enviado do RH para o setor de TI informando quais sistemas o mesmo terá acesso.

Tab 37. Recém contratados - RH

8. Em caso de outros, qual?

Empresa	Resposta
Publica	São encaminhados diretamente ao setor de TI para alteração do cadastro na rede e nos demais sistemas;
Privada	

Tab 38. Recém contratados/Outros – RH

9. Os funcionários que são transferidos de função...

Empresa	Resposta
Publica	São encaminhados diretamente ao setor de TI para alteração do cadastro na rede e nos demais sistemas
Privada	

Tab 39. Funcionários Transferidos - RH

10. Em caso de outros, qual?

Empresa	Resposta
Publica	
Privada	

Tab 40. Recém contratados - RH

4.3.2. SOBRE A DEMISSÃO DE FUNCIONÁRIOS

11. O acesso aos sistemas e à rede dos funcionários demitidos ...

Empresa	Resposta
Publica	Outros
Privada	São bloqueados antes da demissão

Tab 41. Demitidos - RH

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

12. Em caso de outros, qual?

Empresa	Resposta
Publica	São bloqueados após a demissão
Privada	

Tab 42. Demitidos/Outros - RH

13. O acesso dos funcionários demitidos às instalações da empresa...

Empresa	Resposta
Publica	Não é mais permitido
Privada	É restrito à recepção

Tab 43. Acesso físico dos Demitidos - RH

14. Em caso de outros, qual?

Empresa	Resposta
Publica	
Privada	

Tab 44. Acesso físico dos Demitidos/Outros - RH

4.3.3. SOBRE A CONTRATAÇÃO DE TERCEIROS

15. A política de segurança da informação é divulgada sempre na contratação de terceirizados?

Empresa	Resposta
Publica	Não existe política de segurança da informação na empresa
Privada	Sim

Tab 45. Política de segurança aos terceiros - RH

16. Os terceirizados assinam algum termo de responsabilidade e/ou de confidencialidade sobre as informações da empresa?

Empresa	Resposta
Publica	Não
Privada	Não

Tab 46. Termos de responsabilidade aos terceiros - RH

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

17. Os terceirizados recém contratados ...

Empresa	Resposta
Publica	São encaminhados diretamente ao setor de TI para cadastro na rede e nos demais sistemas
Privada	Aguardam o processo de criação de e-mail e senhas após um documento interno ser enviado do RH para o setor de TI informando quais sistemas o mesmo terá acesso

Tab 47. Terceiros recém contratados- RH

18. Observações:

Empresa	Resposta
Publica	-
Privada	-

Tab 48. Observações - RH

4.4. TABULAÇÃO DO QUESTIONÁRIO DA TI

4.4.1. SOBRE A CONTRATAÇÃO/DEMISSÂO DE FUNCIONÁRIOS

1. O cadastro de senha de funcionários novos...

Empresa	Resposta
Publica	Basta o usuário comparecer à TI e solicitar
Privada	Com solicitação por e-mail do Gerente da área

Tab 49. Funcionários novos – TI

2. Os funcionários que são transferidos de função...

Empresa	Resposta
Publica	Solicitam a transferência diretamente à informática
Privada	São transferidos mediante solicitação por e-mail do Gerente da área

Tab 50. Funcionários Transferidos – TI

3. No processo de Demissão de funcionários, a informática...

Empresa	Resposta
Publica	não houve demissão ainda
Privada	A informática faz backup da informação da máquina do usuário antes da demissão.

Tab 51. Demissão de Funcionários – TI

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

4.4.2. SOBRE SENHAS

4. Existe uma política para utilização de senhas fortes?

Empresa	Resposta
Publica	Não
Privada	Não

Tab 52. Política de senhas – TI

5. As senhas de acesso à rede expiram automaticamente em um determinado período de tempo?

Empresa	Resposta
Publica	Sim
Privada	Sim

Tab 53. Expiração de senhas da rede– TI

6. As senhas dos sistemas corporativos são mudadas com que freqüência?

Empresa	Resposta
Publica	Nunca
Privada	Esporadicamente em manutenções do sistema

Tab 54. Política de senhas dos demais sistemas – TI

7. É permitida a utilização de senhas compartilhadas (uma senha única para usuários de um setor por exemplo)?

Empresa	Resposta
Publica	Não
Privada	Não

Tab 55. Senhas compartilhadas – TI

4.4.3. SOBRE TERCEIROS/PRESTADORES DE SERVIÇO

8. Existe algum mecanismo para identificação dos terceiros, prestadores de serviço e funcionários, (Crachá com foto, Uniforme, etc)?

Empresa	Resposta
Publica	Sim
Privada	Sim

Tab 56. Identificação de terceiros – TI

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

9. O atendimento de prestadores de serviço e terceiros é controlado por algum tipo de ordem de serviço com a logomarca da empresa em que ele trabalha?

Empresa	Resposta
Publica	Não
Privada	Não

Tab 57. Controle de Atendimento de terceiros – TI

4.4.4. SOBRE SEGURANÇA DA INFORMAÇÃO

10. Existe uma política de segurança da informação na empresa?

Empresa	Resposta
Publica	Em fase de desenvolvimento
Privada	Em fase de desenvolvimento

Tab 58. Política de Segurança – TI

11. Existem restrições de acesso à Internet e e-mail?

Empresa	Resposta
Publica	Sim
Privada	Sim

Tab 59. Restrições de Acesso – TI

12. Em caso de sim, quais?

Empresa	Resposta
Publica	Sites pornográficos
Privada	Nem todas as máquinas acessam a internet. Existe uma black list com os sites proibidos;

Tab 60. Quais restrições de acesso – TI

13. Os Principais equipamentos de informática (Switches,Servidorer, Roteadores,...) estão realmente protegidos de acesso não autorizado?

Empresa	Resposta
Publica	Parcialmente
Privada	Parcialmente

Tab 61. Proteção de Equipamentos – TI

14. Existe cuidado com o descarte de mídia removível (Documentos impressos, fitas magnéticas, CDR, CDRW entre outros)?

Empresa	Resposta
Publica	Não
Privada	Sim

Tab 62. Descarte d Mídias removíveis – TI

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

15. Utilizam criptografia na comunicação que envolva informações da empresa?

Empresa	Resposta
Publica	Não
Privada	Não

Tab 63. Criptografia – TI

16. Existe antivírus corporativo com atualização automática das estações?

Empresa	Resposta
Publica	Sim
Privada	Sim

Tab 64. Antivírus corporativo – TI

4.4.5. SOBRE COMPUTAÇÃO MÓVEL E TRABALHO REMOTO

17. Os computadores móveis possuem validação de senha antes do acesso ao sistema operacional?

Empresa	Resposta
Publica	Não
Privada	Sim

Tab 65. Senha para computação móvel – TI

18. Os usuários da computação móvel são orientados quanto aos cuidados especiais que devem ter com, por exemplo, atualização de antivírus, acesso não autorizado e divulgação de informações ali armazenadas?

Empresa	Resposta
Publica	Não
Privada	Não

Tab 66. Orientações aos usuários de computação móvel – TI

19. Existe acesso remoto aos sistemas da empresa?

Empresa	Resposta
Publica	Não
Privada	Sim, aos funcionários da empresa

Tab 67. Acesso remoto – TI

20. Se sim, quais os controles utilizados para estes acessos?

Empresa	Resposta
Publica	
Privada	Orientação aos usuários e análise de logs de acesso

Tab 68. Controles para acesso remoto – TI

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

4.5. ANÁLISE DA PESQUISA

A análise da pesquisa foi feita com o intuito de responder a todos os questionamentos levantados na descrição da metodologia, caracterizada de acordo com as informações dos questionários, destacando os pontos fortes e fracos, quando existirem, e ainda comparando por tipo de empresa (Pública e privada).

4.5.1. SOBRE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Em ambas as empresas existem políticas de segurança da informação sendo desenvolvida, porém ainda não está muito claro para os usuários o que é esta política, pois, em média, somente 41,38% dos usuários afirmam a existência da mesma.
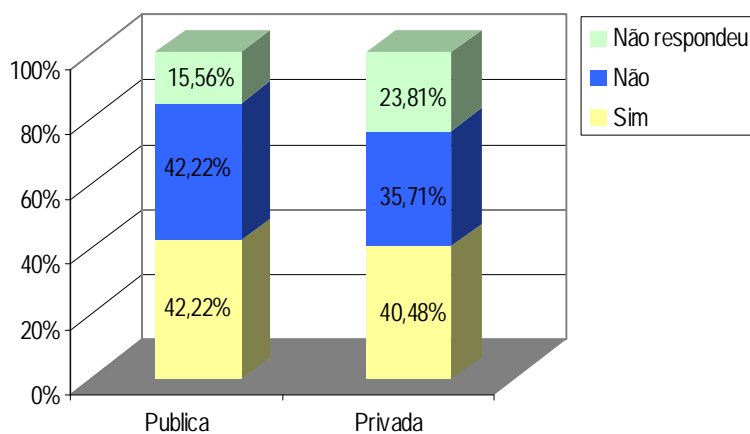
Fig. 1.A empresa possui política de segurança da informação?

A questão de existir uma *política de segurança* em desenvolvimento demonstra consciência da sua necessidade, porém, a falta desta política atualmente é uma das principais falhas no combate aos ataques que utilizam a engenharia social.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

Desta forma, as duas empresas devem Priorizar a finalização da *política de segurança* da informação e garantir a sua divulgação para todos os usuários, através de ações como uma campanha de lançamento, distribuição de folders, informativos, palestras, auditorias internas e outros meios de divulgação e conscientização.

O comprometimento da alta direção é fundamental para a implantação da *política de segurança* da informação. Ela deve estar envolvida em todo o processo e motivar os funcionários.

4.5.2. SOBRE INFORMAÇÕES VITAIS/CONFIDENCIAIS

Para a segurança da informação é fundamental que os usuários conheçam, entre as informações que ele tem acesso, quais são confidenciais e vitais para a continuidade do seu negócio, evitando assim que elas sejam divulgadas ou violadas inadvertidamente.

Na empresa privada 59,52% dos usuários afirmam conhecer as informações consideradas vitais para a empresa, enquanto que na empresa pública, o percentual cai para 40%. Esta consciência deve ser trabalhada, de maneira que cada *usuário* saiba quais informações, dentre as que ele tem acesso, são fundamentais para a empresa.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory
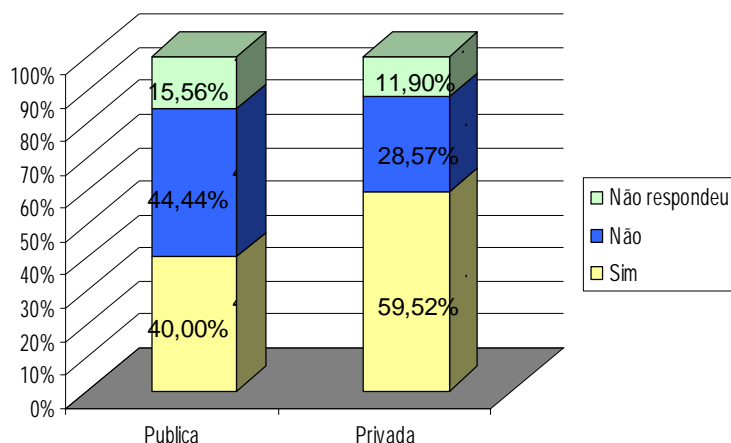
Fig. 2. Os usuários conhecem as informações vitais para a empresa?

Tanto na empresa Privada quanto na empresa pública há um responsável pela comunicação interna e externa. Ele deve ter uma visão sistêmica do impacto causado ao se divulgar uma informação, principalmente uma informação considerada vital e, além disso, deve orientar a forma como as informações são repassadas, de maneira padronizada, tornando este padrão conhecido por todos da empresa.

Dos 87 (oitenta e sete) entrevistados, 86,21% afirmam acessar informações vitais ou informações confidenciais. Desse universo, 18,67% não possuem conhecimento quanto à existência de um responsável pela comunicação interna, sendo que na empresa publica são 26,32% do seu escopo, enquanto que na empresa privada este percentual cai para 10,81%, conforme demonstrado no quadro abaixo.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

Há um responsável pela comunicação interna?	Publica	Privada	TOTAL
Sim	63,16%	72,97%	68,00%
Não	26,32%	10,81%	18,67%
Não respondeu	10,53%	16,22%	13,33%
TOTAL	100%	100%	100%

Fig. 3.Tabela Informações confidenciais / vitais x comunicação interna

Dos usuários que acessam informações confidenciais, menos da metade (47,06%) na empresa pública afirma que a empresa orienta quanto à divulgação de informações e na empresa Privada este percentual sobre para 73,33%.

4.5.3. SOBRE TERMO DE RESPONSABILIDADE

Quando um *usuário* assina um termo responsabilizando-se pela informação, ele será um defensor da segurança desta informação e pensará duas vezes antes de quebrar qualquer procedimento de segurança que ele saiba que existe.

Em ambas as empresas, nem funcionários nem terceiros assinam nenhum termo ou acordo de responsabilidade / confidencialidade.

Em média, nas duas empresas, 73,56% dos usuários têm acesso a informações consideradas confidenciais, dos quais menos da metade (45,31%) afirma saber que as informações são classificadas dentro da empresa e pouco mais da metade deles (aproximadamente 60%) sabem da existência de um responsável pela comunicação externa/Interna e das orientações sobre divulgação da informação.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

Dos usuários que acessam informações confidencias, em ambas as empresas, metade só altera a senha quando o sistema solicita e, praticamente, a outra metade (40,63%) sempre utiliza a mesma senha.

4.5.4. SOBRE SENHAS

As senhas são comumente utilizadas para validar a identificação dos usuários e conceder acesso aos sistemas de informação. Para os engenheiros sociais conseguir uma senha de acesso com um *usuário* é o prêmio que ele mais deseja, pois, desta forma terá acesso às mesmas informações que o *usuário* e o dono da senha será responsabilizado por quaisquer problemas que venham a ocorrer.

Os usuários que têm acesso á informações confidenciais e vitais para a empresa devem ter um cuidado especial, pois são os principais alvos dos ataques contra a segurança da informação. O gráfico da Fig. 4 mostra que, dos usuários que acessam informações confidencias, em ambas as empresas, metade só altera a senha quando o sistema solicita e, praticamente, a outra metade (40,63%) sempre utiliza a mesma senha.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

Fig. 4.Freqüência de alteração de senhas dos usuários com acesso à informações confidenciais

Em ambas as empresas, a grande maioria dos usuários afirma não divulgar as suas senhas, conforme Fig. 5.
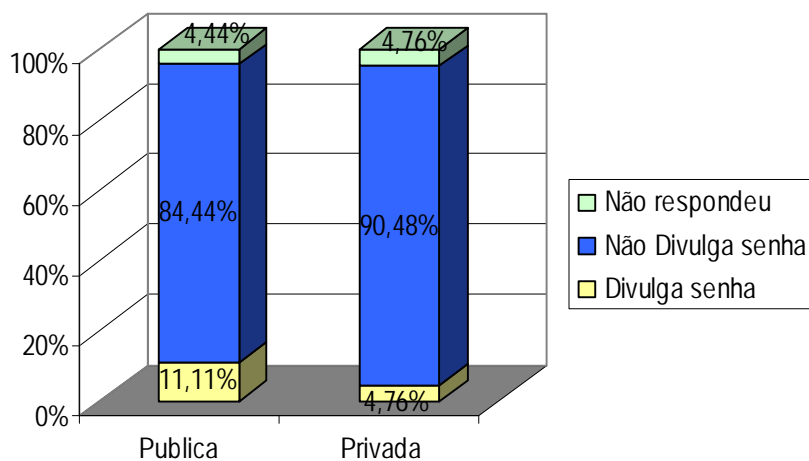
Fig. 5.Quantos usuários divulgam as senhas

Em média, 87,36% dos usuários entrevistados têm suas senhas individuais, não permitindo que outros usuários a conheçam. Na divulgação de

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

senhas, chama a atenção o fato de que 20% dos gerentes da empresa Pública têm sua senha conhecida por outros funcionários e que 32,18% dos usuários deixa que outros utilizem a sua senha para realizar algum trabalho rápido.

Somente 6,90% afirmam anotar suas senhas em algum local próximo ao computador, na agenda ou similar.

Na empresa Pública, 15,56% afirma que sabe a senha de outros usuários, contra 11,90% da empresa Privada.

Dentre usuários que afirmam divulgar e/ou anotar senhas em locais que podem não ser seguros, levantamos quais sistemas de ambas as empresas tem ao menos um funcionário que realiza esta prática, conforme Fig. 6:

Empresa	Sistemas que têm usuários que divulgam senhas	Sistemas que têm usuários que anotam suas senhas
PÚBLICA	- Sistema Financeiro/Contábil - Sistema Orçamentário - Outros sistemas corporativos	- Sistema Financeiro/Contábil - Sistema Orçamentário - Outros sistemas corporativos
PRIVADA	- Sistema de ponto - Folha de Pagamento	- Sistema de ponto - Folha de Pagamento - Sistema com informações gerenciais - Outros sistemas corporativos

Fig. 6. Sistemas com usuários que divulgam/anotam suas senhas em locais de fácil acesso

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

Vemos que os principais sistemas como por exemplo, folha de pagamento , Financeiro/Contábil e alguns sistemas coorporativos, possuem ao menos uma senha compartilhada com mais de um *usuário*.

4.5.5. SOBRE ACESSO ÀS INFORMAÇÕES

Por mais que uma empresa invista em tecnologia para garantir a segurança da informação, é fundamental que os seus usuários participem ativamente com ações, muitas vezes simples, como manter a mesa sem documentos expostos e não deixar um sistema conectado com a sua senha ao sair.

O bloqueio dos computadores é feito pela grande maioria dos usuários, 86,67% na empresa Pública e 71,31% na Privada. O mesmo ocorre com a política de mesa limpa, onde 77,78% dos usuários da empresa Pública e 69,05% da Privada, afirmam ter o costume de deixar a mesa limpa, sem papeis, evitando assim que informações, muitas vezes sigilosas, fiquem expostas.

Praticamente metade dos usuários da empresa Privada (47,62%) acha que não seria difícil que pessoas externas consigam informações importantes da empresa. Na empresa pública, este percentual cai para 33,33%.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

4.5.6. COMPUTAÇÃO MÓVEL E ACESSO REMOTO

Somente a empresa privada afirma utilizar validação de senha antes do acesso ao sistema operacional e nenhuma das duas empresas orienta os usuários da computação móvel quanto aos cuidados como, por exemplo, a atualização de antivírus e acesso de pessoas não autorizadas, incluindo parentes e amigos.

Somente a empresa privada faz acesso remoto aos seus sistemas e já realiza a orientação aos usuários e analisa os logs de acesso.

4.5.7. PROCESSOS DO RH

É necessário, em ambas as empresas, uma ação de *procedimentar* os principais processos que envolvem riscos à segurança da informação, como por exemplo todos os processos onde há uma interação com o setor responsável pela tecnologia da informação, como no caso de contratação, demissão e transferência de funcionários e terceiros onde, temos falhas como:

1. Na empresa Pública, basta que o *usuário* compareça à área de *TI* informando que é um novo funcionário para que seja criada uma senha de acesso à rede e aos sistemas;

2. Na empresa Privada, a *TI* libera o acesso com uma requisição do gerente da área, enquanto que o RH informa que é necessário um documento do

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

RH para a *TI*, informando quais sistemas o funcionário novo, transferido ou Terceirizado irá acessar.

Além do termo de responsabilidade, o RH deve solicitar a assinatura de termos como o de utilização de e-mail e Internet, de confidencialidade de senhas e, principalmente realizar treinamentos da *política de segurança*, assim que o funcionário é admitido.

Ações como estas permitirão uma maior contribuição do setor de RH em ambas as empresas, minimizando os riscos de falhas na segurança da informação.

4.5.8. PROCESSOS DA TI

A área de *TI* deve ter uma atuação decisiva no processo de segurança da informação. Vários controles podem ser implementados para minimizar os riscos sobre a segurança da informação e abaixo citamos os controles existentes no ambiente estudado:

Controle de senhas: A expiração automática de senhas de aceso á rede, em um período pré-definido, que já é utilizado em ambas as empresas. Porém, deve-se atentar para situações como as dos sistemas corporativos, que, na empresa Pública, nunca mudam as senhas e, na empresa privada, mudam somente esporadicamente nas manutenções dos sistemas.

Controle sobre prestadores de serviços e terceiros: Apesar dos prestadores de serviços e terceiros possuírem mecanismos de identificação como

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

crachás com fotos, senhas, ou uniformes, não existe um controle sobre os serviços executados, através de uma ordem de serviço, por exemplo.

Controle no acesso à Internet: Existe algum controle de acesso à Internet, como por exemplo uma lista de usuários com acesso negado (Black list) ou o bloqueio a sites pornográficos.

Controle de segurança dos equipamentos: Em ambas as empresas existe um controle parcial sobre o acesso não autorizado. É necessário realizar um levantamento mais detalhado de quais são os equipamentos que não estão protegidos .

Antivírus: Em ambas as empresas existe um antivírus coorporativo implementado.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

4.6. SOLUÇÕES PROPOSTAS

Como vimos, existem diversas técnicas que podem ser utilizadas em ataques de engenharia social e todas elas usam a boa fé e a ingenuidade das pessoas, conquistando sua confiança para conseguir quebrar a segurança.

Ainda nos dias de hoje, a visão de segurança da informação está atrelada apenas a tecnologia, esquecendo que por trás de cada máquina há pelo menos uma pessoa. Implantar controles de segurança exige uma estrutura complexa de pessoas, meios e processos, interagindo de maneira a preservar a confidencialidade, integridade e disponibilidade das informações.

Mitnick (2003, p. 4) diz que "A segurança não é um produto, ela é um processo." Para ele, a grande maioria das empresas investe em ferramentas que ajudam somente na proteção dos intrusos amadores, que em sua maioria são crianças (*script kiddies*) que só causam aborrecimento. Elas não estão realmente protegidas contra os atacantes sofisticados, com alvos bem definidos e motivados pelo ganho financeiro.

4.6.1. CONTROLES SUGERIDOS

Para minimizar os riscos da segurança da informação, baseados na análise da pesquisa aplicada, sugerimos alguns controles que podem ser implementados tanto na empresa Pública quanto na Privada, são eles:

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

4.6.2. IMPLANTAÇÃO DE UMA POLÍTICA DE SEGURANÇA

A finalização da política de segurança é fundamental e prioritário para as duas empresas estudadas. Ela deve ser elaborada com a participação do RH e da *TI*, baseando-se nas melhores práticas da norma NBR ISO 17799, divulgando para todos os funcionários na contratação (através do RH) e em meio eletrônico com por e-mail e na intranet (gerenciado pela *TI*). Ela deve abordar questões como a privacidade, direitos de acesso, responsabilidades e deve refletir os objetivos do negócio além de estar de acordo com a cultura organizacional de cada empresa.

É importante frisar que deve ser avaliado o custo da implantação de tal política, para que não seja superior ao valor da informação que se está protegendo, levando-se em conta fatores, como por exemplo a imagem da empresa em caso de uma falha na segurança da informação.

4.6.3. NA ADMISSÃO E DEMISSÃO DE FUNCIONÁRIOS

Em nenhuma das empresas existe um procedimento padrão e seguro para contratar, demitir ou transferir usuários. Convém que os usuários assinem termos de responsabilidade e/ou acordos de confidencialidade ou não divulgação no início da sua contratação ou antes do acesso às instalações de processamento da informação [13]. As responsabilidades e direitos legais dos usuários devem ser claros e formais, sendo recomendado que sejam inseridos dentro dos termos e condições de trabalho;

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

O RH deve checar as informações contidas nos currículos e os certificados dos cursos apresentados pelos candidatos pré-selecionados para uma contratação, para confirmar a veracidade das informações. No caso da empresa Pública, deve-se avaliar se o funcionário está apto a exercer a função que lhe assiste e tomar as providencias cabíveis como transferência de função ou treinamento.

A área de *TI* deve criar, transferir ou bloquear um *usuário*, somente com uma autorização do responsável pela contratação, em geral do RH, por escrito, com todas as informações necessárias, como nome completo, setor de destino, função, entre outros. Até que o novo acesso seja liberado, o futuro *usuário* não deve utilizar senha de nenhum outro funcionário.

No caso da demissão, o responsável pelo bloqueio de senhas no setor de *TI* deve ser comunicado antes do *usuário* que será demitido, para que as devidas providências de segurança sejam tomadas, de acordo com a prática da empresa, seja ela bloquear o *usuário*, fazer backup dos dados, alterar o acesso para somente leitura, etc.

4.6.4. POLÍTICA DE SENHAS FORTES

Nenhuma das empresas utiliza uma política de senhas fortes e nem orienta seus usuários neste sentido. Esta política deve estar inserida na *política de segurança* da informação e conter pelo menos as condições a seguir:

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

- As senhas devem ser únicas e individuais, permitindo a identificação de cada *usuário* e responsabilizando–o por suas ações, .

- Os usuários devem estar cientes, formalmente, que devem manter a confidencialidade de sua(a) senha(s), através de um documento escrito sobre seus direitos de acesso;

- As senhas devem expirar automaticamente em um período pré-definido, solicitando que o usuário altere-a de maneira que ele não possa repetir senhas antigas e seja obrigado a misturar, no mínimo, letras e números;

- As senhas dos sistemas coorporativos devem ser alteradas com uma determinada freqüência.

4.6.5. TREINAMENTO DOS USUÁRIOS

Visando assegurar que os usuários estão cientes das ameaças e transformá-los em defensores da segurança da informação, eles devem ser treinados nos procedimentos de segurança e no uso correto das instalações da empresa. Isso inclui os prestadores de serviço e terceiros.

Como já foi dito neste trabalho, não importa o valor que uma empresa invista em tecnologia para a segurança da informação, pois a cooperação dos usuários autorizados é fundamental para eficácia da segurança

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

4.6.6. CONTROLE NO ACESSO DE TERCEIROS

Para o controle de acesso de terceiros e/ou prestadores de serviço, deve-se verificar o tipo de acesso (Lógico ou físico), as razões para acesso, questões relativas a confidencialidade das informações (conforme controle sugerido na contratação, demissão e transferência de funcionários e terceiros).

Para o acesso físico interno, deve-se verificar a utilização de uma identificação que permita rápida confirmação de identidade como um crachá com foto e se possível o uso de um uniforme e a execução de um serviço deve ser acompanhada por um documento com a logomarca da empresa (Ordem de serviço), contendo no mínimo o motivo da intervenção, a data, a hora e o nome do técnico;

Deve estar claro, e em contrato, a questão sobre definição de responsabilidade (Em caso de acidentes) e, antes de qualquer acesso às instalações, os técnicos devem ser treinados nos procedimentos de segurança;

4.6.7. RESTRIÇÕES DE ACESSO A E-MAIL E INTERNET

Existem pequenas medidas de restrições de acesso á Internet, em ambas empresas, que utilizam a tecnologia, mas não existe nenhum termo de uso de e-mail e Internet para orientação e conscientização dos usuários.

A criação de um termo que regulamenta o uso do e-mail e Internet é fundamental e deve ser incluída na política de segurança da informação. Ele deve

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

incluir proteção de anexos, orientação de quando não se deve utilizá-los, responsabilidade sobre o uso indevido, uso de criptografia em mesagens com informações da empresa, entre outros. Além disso, a *TI* deve monitorar os acessos à Internet e bloquear os acessos a sites que não agregam valor ao negócio.

4.6.8. SEGURANÇA FÍSICA AOS EQUIPAMENTOS VITAIS

Em ambas as empresas os principais equipamentos que podem por em risco a segurança da informação (Servidores, switchs, entre outros) só estão parcialmente protegidos do acesso a pessoas não autorizadas.

Deve-se realizar um levantamento de todos os equipamentos críticos e definir a melhor maneira para protegê-los, verificando inclusive a necessidade de Implementação de mecanismos de segurança física como por exemplo circuitos fechados de TV e fechaduras eletrônicas.

4.6.9. DESCARTE DE MÍDIAS REMOVÍVEIS

Informações importantes podem ser divulgadas através da eliminação de mídias de maneira descuidada. A empresa privada afirma ter um cuidado com o descarte de mídias removíveis, mas não informa quais. Sugerimos a utilização de um triturador de papel em áreas com informações consideradas confidenciais como a *T.I.* e o RH, além de um controle sobre as mídias removíveis, desabilitando este recurso nas máquinas que não devem utilizá-lo, além da orientação aos usuários na utilização das mesmas.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

Pode-se criar uma coleta de descarte seguro, de maneira que todas as mídias removíveis a serem inutilizadas sejam encaminhadas para um responsável pelo descarte seguro das mesmas.

4.6.10. CRIPTOGRAFIA

Não existe cultura de utilização da criptografia em nenhuma das empresas. Sugerimos que esta cultura seja inserida em ambas as empresas de forma gradativa, iniciando com um grupo de usuários, sugerimos a *T.I.*, e em seguida seja expandido para outros usuários, como os que utilizam notebook, os do RH e os demais usuários que trocam informações confidenciais das empresas.

4.6.11. COMPUTAÇÃO MÓVEL E ACESSO REMOTO

Cuidados especiais são necessários para a utilização de computação móvel. Convém que os usuários sejam formalmente alertados dos riscos para a segurança da informação com a computação móvel.

Alguns controles podem ser implementados como precaução para diminuir estes riscos, como a orientação de que o usuário sempre mantenha o equipamento longe de acesso de pessoas não autorizadas como parentes e visinhos, atualize seu antivírus freqüentemente, utilização de senha na inicialização

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

do equipamento, cuidados contra roubo dos equipamentos e o uso freqüente da criptografia em arquivos com informações da empresa;

Para a empresa privada que utiliza acesso remoto, o acesso remoto deve ser autorizado e controlado o desenvolvimento de políticas, procedimentos e normas específicas, que abordem questões como por exemplo, qual trabalho é permitido, as horas de trabalho e o acesso de pessoas não autorizadas ao equipamento de onde se faz o acesso remoto.

4.6.12. CONTROLES GERAIS

Para minimizar os riscos de roubo e exposição de informações, ambas instituições, devem adotar a política de mesa limpa em toda a instituição, principalmente na empresa pública, onde o percentual de usuários que tem esse costume é menor. Sugerimos que seja feito uma sensibilização para que os usuários mantenham à vista somente os papeis que estão sendo utilizados no momento, bloqueiem os terminais quando não estiverem em uso, informações impressas devem ser retiradas imediatamente da impressora e, ao saírem da empresa, mantenham os micros desligados e os papeis com informações confidenciais em gavetas adequadas, preferencialmente com fechadura.

Todos os usuários devem estar cientes, formalmente, que equipamentos, informações ou softwares são de propriedade da empresa e não devem ser retirados da mesma sem autorização.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

4.6.13. FÓRUM DE SEGURANÇA

O processo de segurança da informação é responsabilidade de todos os usuários da direção da empresa, porém, é natural que, ao menos nas empresas estudadas, os setores de RH e TI liderem a implantação dos controles citados.

Desta forma, com base na norma NBR ISO 17788, sugerimos que seja criado um fórum de gestão da segurança da informação, multifuncional onde os setores mais relevantes na empresa estejam representados. Seu principal objetivo é de garantir uma implantação adequada, realizando análises críticas e monitoração necessárias para que a segurança seja parte de todo e qualquer processo na empresa.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

5. CONCLUSÃO

O procedimento proposto neste trabalho nos permitiu realizar um levantamento da atual consciência dos usuários, quanto à importância da informação acessada pelos mesmos, de maneira que o impacto da engenharia social na segurança da informação pôde ser avaliado com base na análise dos questionários aplicados.

Alinhado à análise da consciência dos usuários, foram analisados os processos das áreas de recursos humanos e de tecnologia da informação, no que diz respeito à engenharia social. Toda a análise foi realizada em duas empresas com características diferentes, permitindo assim que o procedimento criado possa ser utilizado em vários tipos de empresas, independente de suas características.

Após a análise da pesquisa, utilizamos a norma NBR ISO 17799, Código de Prática para Gestão da segurança da Informação, como base para propor um leque de controles que visam minimizar as falhas de segurança da informação e os riscos de ataques bem sucedidos de engenharia social, aumentando a segurança nas pessoas e conscientizando seus usuários da importância da informação da empresa para que eles cumpram seu papel de agentes da segurança da informação.

Porém este trabalho limita-se apenas ao diagnóstico do problema. As ações necessárias à implantação dos controles são de responsabilidade de cada empresa que, após este trabalho, já estão com os seus pontos críticos na segurança

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

da informação identificados e, para cada um deles, existe aqui um ou mais controles que visam eliminar as falhas existentes.

Muitas empresas investem nas melhores tecnologias de segurança e, muitas vezes esquecem de tratar o elo mais fraco na segurança da informação: o fator humano. Desta forma, a metodologia utilizada neste trabalho permite que empresas implementem controles que minimizem o risco de ataques de engenharia social com um baixo custo.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

6. ANEXOS

6.1.ANEXO I – QUESTIONÁRIO APLICADO AOS USUÁRIOS

PESQUISA SOBRE A SEGURANÇA DA INFORMAÇÃO
ARACAJU, ____ / ____ DE 2004

SOBRE O FUNCIONÁRIO

1.Faixa etária
a) [ ]Até 20 anos
b) [ ]De 21 a 30 anos
c) [ ]De 31 a 40 anos
d) [ ]Acima de 40

2.Sexo
a) [ ]Masculino
b) [ ]Feminino

3.Função
a) [ ]Gerencial (Chefe de divisão, Chefe de Gabinete, Diretoria, etc...)
b) [ ]Operacional (Agente administrativo, Oficial administrativo, Auxiliar de Gabinete, etc...)
c) [ ]Terceirizados (Prestadores de Serviços, estagiários, etc...)

4.Trabalha na EMPRESA a
a) [ ]Menos de 1 ano
b) [ ]De 1 a 5 anos
c) [ ]De 6 a 10 anos
d) [ ]Acima de 10 anos

5.Possui outro emprego?
a) [ ]Sim, na mesma área em que trabalho na EMPRESA
b) [ ]Sim, em outra área
c) [ ]Não

SOBRE SENHAS

6.Alguém, além de você, sabe a(s) sua(s) senha(s) utilizada(s) para acessar informações da EMPRESA? [ ] Sim [ ] Não

7.Você utiliza a senha de algum outro funcionário para acesso à informações da EMPRESA?
[ ] Sim [ ] Não

8.Você anota as suas senhas em algum local próximo ao computador, na agenda, ou local similar?
[ ] Sim [ ] Não

9.Você deixa outras pessoas utilizarem sua senha para algum trabalho rápido? [ ] Sim [ ] Não

10.Com que freqüência você altera (s) sua(s) senha(s):
a) [ ]Mensalmente
b) [ ]Trimestralmente
c) [ ]Semestralmente
d) [ ]Somente quando o sistema solicita alteração
e) [ ]Sempre utilizo mesma senha

SOBRE DIVULGAÇÃO DE INFORMAÇÕES

11.Como você procede para fornecer informações, que você tem acesso, solicitadas por telefone ou e-mail?
a) [ ]Forneço a informação, pois não há nada confidencial em minha área.
b) [ ]Forneço a informação após identificar o solicitante
c) [ ]Solicito autorização a meu superior para liberar a informação;
d) [ ]Outros:
____

SOBRE A EMPRESA

12. A EMPRESA possui política de comunicação interna?[ ] Sim [ ] Não
13. As informações são classificadas na EMPRESA (confidencial, secreta, pública etc.) [ ] Sim [ ] Não
14. A EMPRESA possui um responsável pela comunicação externa?[ ] Sim [ ] Não
15. A EMPRESA possui alguma orientação quanto à divulgação de informação?[ ] Sim [ ] Não
16. Você sabe quais as informações são vitais para o negócio da EMPRESA?[ ] Sim [ ] Não
17. A EMPRESA possui política de segurança da informação?[ ] Sim [ ] Não

SOBRE ACESSO À INFORMAÇÃO

18. Neste momento existe algum papel sobre sua mesa com informações sobre a EMPRESA?
[ ] Sim [ ] Não

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

19. Ao sair você costuma deixar suas mesa limpa, sem papéis?
[ ] Sim [ ] Não
20. Ao sair você costuma deixar seu computador bloqueado ou efetuar o LogOff?
[ ] Sim [ ] Não
21. O seu setor possui informações consideradas confidenciais?
[ ] Sim [ ] Não
22. Na sua opinião, todos os funcionários do seu setor sabem a importância das informações da EMPRESA?
[ ] Sim [ ] Não
23. Na sua opinião, seria difícil pessoas externas conseguirem informações importantes na EMPRESA?
[ ] Sim [ ] Não
24.Quais os tipos de informações que você tem acesso?
a) [ ]Informações operacionais
b) [ ]Informações gerenciais
c) [ ]Informações confidenciais
d) [ ]Informações imprescindíveis à continuidade do negócio
e) [ ]Não tenho acesso a nenhuma informação importante

SOBRE OS SISTEMAS UTILIZADOS

25.Dos sistemas abaixo, quais você utiliza?
a) [ ]Sistema de Ponto
b) [ ]Sistema Financeiro e/ou Contábil
c) [ ]Sistema de Patrimônio
d) [ ]Folha de Pagamento
e) [ ]Sistema orçamentário
f) [ ]Sistemas com informações gerenciais
g) [ ]Outros___________________________________
____

OBSERVAÇÕES

26. Qualquer observação sobre alguma resposta, favor informar o nº da questão e a Observação:
____
____
____
____
____
____
____
____
____
____
____
____
____

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

6.2.ANEXO-II QUESTIONÁRIO APLICADO AO RH

PESQUISA SOBRE A SEGURANÇA DA INFORMAÇÃO APLICADA AO RH
ARACAJU, ____ / ____ DE 2004

SOBRE A CONTRATAÇÃO DE FUNCIONÁRIOS

1. A política de segurança da informação é divulgada aos novos contratados?
a) [ ]Sim
b) [ ]Não
c) [ ]Não existe política de segurança da informação na empresa
2. Os funcionários assinam algum termo de responsabilidade e/ou de confidencialidade sobre as informações da empresa?
a) [ ]Sim
b) [ ]Não
3. Existe alguma orientação de restrição quanto à utilização de e-mail, Internet ou telefone?
a) [ ]Sim, por escrito e assinada;
b) [ ]Sim, através do Servidor da rede e da central telefônica
c) [ ]Não existe
d) [ ]Outros
4. Em caso de outros, qual?

___

5. As informações (geralmente contidas no currículo) dos candidatos, fornecidas no processo de seleção, são checadas antes da contratação?
a) [ ]Sim
b) [ ]Não
c) [ ]Outros
6. Em caso de outros, qual?

___

7. Os funcionários recém contratados ...

a) [ ]Acessam os sistemas e a rede utilizando as senhas de outros funcionários até que as suas sejam criadas;

b) [ ]São encaminhados diretamente ao setor de TI para cadastro na rede e nos demais sistemas;
c) [ ]Aguardam o processo de criação de e-mail e senhas após um documento interno ser enviado do RH para o setor de TI informando quais sistemas o mesmo terá acesso;
d) [ ]Têm seus nomes e funções informados ao setor de TI, via e-mail ou fax, para providencias de senhas;
e) [ ]Outros
8. Em caso de outros, qual?

___

9. Os funcionários que são transferidos de função...
a) [ ]Acessam os sistemas e a rede utilizando as senhas de outros funcionários até que seu novo acesso seja liberado;
b) [ ]São encaminhados diretamente ao setor de TI para alteração do cadastro na rede e nos demais sistemas;
c) [ ]Aguardam o processo de alteração de acesso, após um documento interno ser enviado do RH para o setor de TI solicitando a transferência;
d) [ ]Têm seus nomes e funções (novas e antigas) informados ao setor de TI, via e-mail ou fax, para providencias de bloqueio e liberação de acesso.
e) [ ]Outros
10.Em caso de outros, qual?

___

___

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

SOBRE A DEMISSÃO DE FUNCIONÁRIOS

11.O acesso aos sistemas e à rede dos funcionários demitidos ...
a) [ ]São bloqueados antes da demissão;
b) [ ]São bloqueados após o funcionário remover seus arquivos pessoais da rede;
c) [ ]Nunca são bloqueados;
d) [ ]Outros
12.Em caso de outros, qual?

____

13. O acesso dos funcionários demitidos às instalações da empresa...
a) [ ]Continua o mesmo sem restrições;
b) [ ]É restrito à recepção;
c) [ ]Não é mais permitido
d) [ ]Outros
14.Em caso de outros, qual?

____

____

SOBRE A CONTRATAÇÃO DE TERCEIROS

15.A política de segurança da informação é divulgada sempre na contratação de terceirizados?
a) [ ]Sim
b) [ ]Não
c) [ ]Não existe política de segurança da informação na empresa
16.Os terceirizados assinam algum termo de responsabilidade e/ou de confidencialidade sobre as informações da empresa?
a) [ ]Sim
b) [ ]Não
17.Os terceirizados recém contratados ...
a) [ ]Acessam os sistemas e a rede utilizando as senhas de outros funcionários até que as suas sejam criadas;
b) [ ]São encaminhados diretamente ao setor de TI para cadastro na rede e nos demais sistemas;
c) [ ]Aguardam o processo de criação de e-mail e senhas após um documento interno ser enviado do RH para o setor de TI informando quais sistemas o mesmo terá acesso;
d) [ ]Têm seus nomes e funções informados ao setor de TI, via e-mail ou fax, para providencias de senhas;
e) [ ]Outros

OBSERVAÇÕES

18. Qualquer observação sobre alguma resposta, favor informar o nº da questão e a Observação:

____

____

____

____

____

____

____

____

____

____

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

6.3.ANEXO-III QUESTIONÁRIO APLICADO À INFORMÁTICA

PESQUISA SOBRE A SEGURANÇA DA INFORMAÇÃO APLICADA À TI
ARACAJU, ____ / ____ DE 2004

SOBRE A CONTRATAÇÃO/DEMISSÃO DE FUNCIONÁRIOS

1. O cadastro de senha de funcionários novos...

a) [ ]Basta que o usuário compareça à sala da informática solicitando a criação da senha;
b) [ ]É realizado mediante solicitação por e-mail do Gerente da área;
c) [ ]Somente após um documento interno ser enviado do RH para o setor de TI informando quais sistemas o mesmo terá acesso;
d) [ ]Outros

2. Em caso de outros, qual?

____

____

3. Os funcionários que são transferidos de função...

a) [ ]Solicitam a transferência diretamente à informática;
b) [ ]São transferidos mediante solicitação por e-mail do Gerente da área;
c) [ ]Aguardam o processo de alteração de acesso, após um documento interno ser enviado do RH para o setor de TI solicitando a transferência;
d) [ ]Outros

4. Em caso de outros, qual?

____

____

5. No processo de Demissão de funcionários, a informática...

a) [ ]Bloqueia os acessos à rede e dos sistemas corporativos antes da demissão;
b) [ ]Os acessos são bloqueados após o funcionário remover seus arquivos pessoais da rede;
c) [ ]Os acessos nunca são bloqueados;
d) [ ]Outros

6. Em caso de outros, qual?

____

____

SOBRE SENHAS

7. Existe uma política para utilização de senhas fortes?
   [ ] Sim, ainda não divulgada;
   [ ] Sim, em pleno funcionamento
   [ ] Não
8. As senhas de acesso à rede expiram automaticamente em um determinado período de tempo?
   [ ] Sim [ ] Não
9. As senhas dos sistemas corporativos são mudadas com que freqüência?

a) [ ]Mensalmente
b) [ ]Trimestralmente
c) [ ]Semestralmente
d) [ ]Esporadicamente em manutenções do sistema
e) [ ]Nunca

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

10. É permitida a utilização de senhas compartilhadas (uma senha única para usuários de um setor por exemplo)?
    [ ] Sim [ ] Não

SOBRE TERCEIROS/PRESTADORES DE SERVIÇO

11. Existe algum mecanismo para identificação dos terceiros, prestadores de serviço e funcionários, (Crachá com foto, Uniforme, etc)?

a) [ ] Sim;
b) [ ] Não;

12. O atendimento de prestadores de serviço e terceiros é controlado por algum tipo de ordem de serviço com a logomarca da empresa em que ele trabalha??

a) [ ] Sim;
b) [ ] Não;

SOBRE SEGURANÇA DA INFORMAÇÃO

13. Existe uma política de segurança da informação na empresa?

a) [ ]Sim
b) [ ]Não
c) [ ]Em fase de desenvolvimento

14. Existem restrições de acesso à Internet e e-mail?

a) [ ]Sim
b) [ ]Não

15. Em caso de sim, quais?

____

____

16. Os Principais equipamentos de informátIca (Switches,Servidorer, Roteadores,...) estão realmente protegidos de acesso não autorizado?

a) [ ]Sim;
b) [ ]Parcialmente;
c) [ ]Não;

17. Existe cuidado com o descarte de mídia removível (Documentos impressos, fitas magnéticas, CDR, CDRW entre outros)?

a) [ ]Sim;
b) [ ]Não;

18. Utilizam criptografia na comunicação que envolva informações da empresa?

a) [ ]Sim;
b) [ ]Não;

19. Existe antivírus corporativo com atualização automática das estações?

a) [ ]Sim;
b) [ ]Não;

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

SOBRE COMPUTAÇÃO MÓVEL E TRABALHO REMOTO
20. Os computadores móveis possuem validação de senha antes do acesso ao sistema operacional? a) [ ]Sim; b) [ ]Não; c) [ ]Não há computadores móveis 21. Os usuários da computação móvel são orientados quanto aos cuidados especiais que devem ter com, por exemplo, atualização de antivírus, acesso não autorizado e divulgação de informações ali armazenadas? a) [ ]Sim; b) [ ]Não; c) [ ]Não há usuários de computação móvel 22. Existe acesso remoto aos sistemas da empresa? a) [ ]Sim, aos funcionários; b) [ ]Sim, para terceiros; c) [ ]Não; 23. Se sim, quais os controles utilizados para estes acessos? a) [ ]Alterações de senhas com maior freqüência; b) [ ]Orientação aos usuários; c) [ ]Definição de horários para acesso; d) [ ]Análise de logs de acesso; e) [ ]Nenhum
OBSERVAÇÕES

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

6.4.ANEXO III – CRONOGRAMA

Atividade	Nov	Dez	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez	Jan	Fev	Mar	Abr	Mai	Jun	Jul
Levantamento bibliográfico																					
Elaboração do Projeto																					
Elaboração dos Questionários																					
Aplicação dos questionários																					
Estudo dos Processos do RH																					
Avaliação da Pesquisa																					
Criação dos Controles e Ações																					
Elaboração do Relatório Final																					
Apresentação																					

* Início do projeto: Nov de 2003.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

7. GLOSSÁRIO

Biometria

Sistema de identificação de usuários que utiliza características físicas, como por exemplo a impressão digital, a íris, a voz entre outros.

Cavalos de Tróia

Programas que são aparentemente inofensivos, mas que, ao serem executados, iniciam de forma escondida, ataques ao sistema.[16]

Engenheiro social

Geralmente Hackers que tentam ganhar a confiança dos usuários no intuito de conseguir informações úteis em seus ataques. Tentam se passar por um usuário autorizado e ganhar o acesso ilícito aos sistemas. [16]

Hackers

Pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros. [16]

internet banking

É a Home Page de um banco. O site onde são oferecidos basicamente os mesmos serviços de uma agencia bancária. Através do site de um banco um cliente pode realizar transferências bancárias, pagamentos, etc.

Malware

Os vírus, trojans, worms , entre outros, são batizados a genericamente de Malwares;

Política de Segurança

O conjunto das leis, diretrizes, regras, e das práticas que regulam como uma organização controla, protege, e distribui a sua informação.[16]

Procedimentar:

Padronizar uma ação ou um processo em documento oficial.

Script kiddies

São, em geral, adolescentes que utilizam ferramentas e “receitas prontas” para ataques virtuais. Atacam somente pela curiosidade e muitas vezes não estão interessados em pegar informações, mas sim por a prova seus conhecimentos.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

Smart cards

Cartão semelhantes aos cartões de créditos e que geralmente são utilizados na identificação do usuário para controle de acesso, convênios médicos e também como dinheiro eletrônico.

Spywares

Spyware geralmente é incluído na instalação de algum outro software gratuito. Tem o objetivo de coletar informações sem o conhecimento do usuário, e enviá-las para anunciantes ou para o desenvolvedor do software. Ele pode coletar e transmitir informações sobre teclas pressionadas, hábitos de navegação na Web, senhas, endereços de e-mail entre outros.

TI

Sigla que significa Tecnologia da informação. Aqui é citado como sendo o setor responsável em manter a tecnologia utilizada na empresa de maneira a garantir que a informação esteja disponível e segura para todos que possuem acesso à mesma. Corresponde ao então setor de informática.

Usuário

Pessoa que opera um microcommputador, que tem acesso á informações da empresa através e que faz parte do escopo deste projeto.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

8. REFERENCIAS BIBLIOGRÁFICAS

[1] NORMA ISO/IEC 17799. **Código de Prática para Gestão da segurança da Informação nas Empresas**. ABNT – Associação Brasileira de Normas Técnicas. 01 de dezembro de 2000.

[2] LIMA, MAYKA DE SOUZA. **Metodologia para Desenvolvimento de Políticas de Segurança**. Aracaju,2001. 152p. Monografia de Graduação de curso de Ciência da Computação. UNIT- Universidade Tiradentes, 2001.

[3] WADLOW, Thomas A. **Segurança de Redes :** Projeto e gerenciamento de redes seguras. Tradução : Fábio Freitas da Silva. Rio de Janeiro : Campus, 2000. 269 p.

[4] COMER, Douglas E. **Interligação em redes com TCP/IP:** Princípios, protocolos e arquitetura. Tradução : ARX Publicações. Rio de Janeiro : Campus, 1998. 672 p.

[5] MCCARTTHY, Mary pat; CAMPBELL, Stuart. **Transformação na Segurança Eletrônica:** Estratégia e gestão da Defesa Digital. Tradução: Celso Roberto Paschoa. São Paulo: Pearson Education do brasil, 2003. 184 p.

[6]Agencia Folha **Entrevista com Kevin Mitnick**. Disponível em: < http://www1.folha.uol.com.br/folha/informatica/ult124u13942.shtml>. Acesso em: 08 de novembro de 2003.

[7] MODULO SECURITY SOLUTIONS. **Ameaça além do firewal:** Por que as empresas devem se preparar contra a Engenharia social. Disponível em: <www.modulo.com.br>. Acesso em: 08 de novembro de 2003.

[8] MITNICK, Kevin D.; SIMON, William L. A. **A arte de Enganar:** Ataque de Hackers: Controlando o Fator Humano na Segurança da Informação. Tradução : Kátia Aparecida Roque. São Paulo: Pearson Education do brasil, 2003. 278 p.

[9] CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e de informação**. São Paulo: Administração regional do SENAC , 1999. 367 p.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory

[10] ZORRINHO, C. (1995)-**Gestão da Informação. Condição para Vencer**. Iapmei pg.15.

[11]. Computarword. **O Brasil ainda investe pouco em segurança da informação**. Disponível em: <http://idgnow.terra.com.br/idgnow/corporate/2002/04/0033>. Acesso em: 24 de abril de 2004.

[12] SCHNEIER, Bruce. **Segurança .com:** Segredos e mentiras sobre a proteção na vida digital. Rio de janeiro: Campus, 2001. 403 p.

[13] NORMA NBR ISO/IEC 17799. **Código de Prática para Gestão da segurança da Informação nas Empresas**: itens 6.1.3 e 6.1.4. ABNT – Associação Brasileira de Normas Técnicas. 01 de dezembro de 2000.

[14] NORMA ISO/IEC 17799. **Código de Prática para Gestão da segurança da Informação nas Empresas**: itens 2.1 ABNT – Associação Brasileira de Normas Técnicas. 01 de dezembro de 2000.

[15] MODULO SECURITY SOLUTIONS. **Ferramenta gratuita ajuda usuários no combate às fraudes de internet**. Disponível em: http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=7&objid=3139&pagenumber=0&idiom=0. Acesso em: 27 de julho de 2004.

[16] MODULO SECURITY SOLUTIONS. **Glossário**. Disponível em: http://www.modulo.com.br/pt/page_i.jsp?page=50&tipoid=12&pagecounter=0. Acesso em: 27 de julho de 2004.

PDF criado com versão de teste do pdfFactory Pro. Para comprar, acesse www.divertire.com.br/pdfFactory